BLOCKCHAIN И КРИПТОВАЛЮТЫ

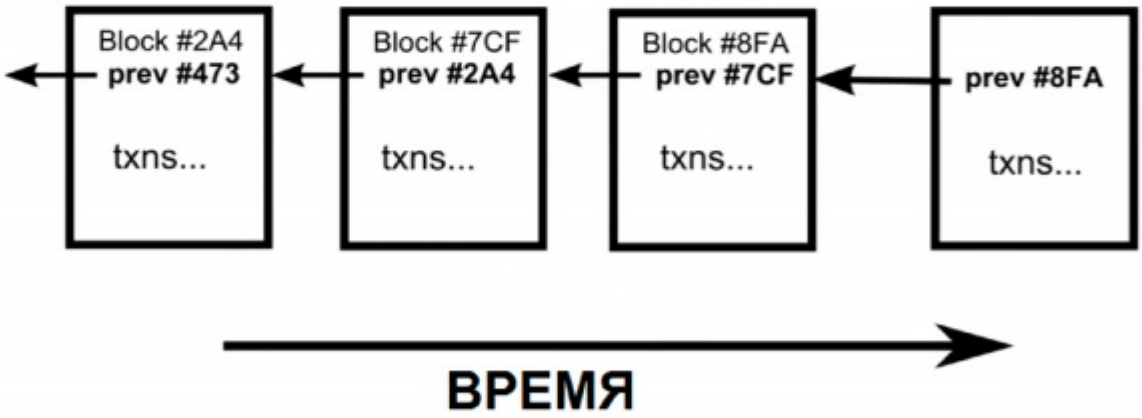
BlockChain (цепочка блоков) – это технология надежного распределенного хранения записей данных, в принципе, о чём угодно. В большинстве случаев эти записи описывают минимально логически осмысленные операции – транзакции.

Транзакции бывают двух типов:

- транзакции ввода,
- транзакции вывода.

Касательно финансовых операций транзакциями ввода будут операции по зачислению средств на счёт, транзакциями вывода – списания денег со счёта.

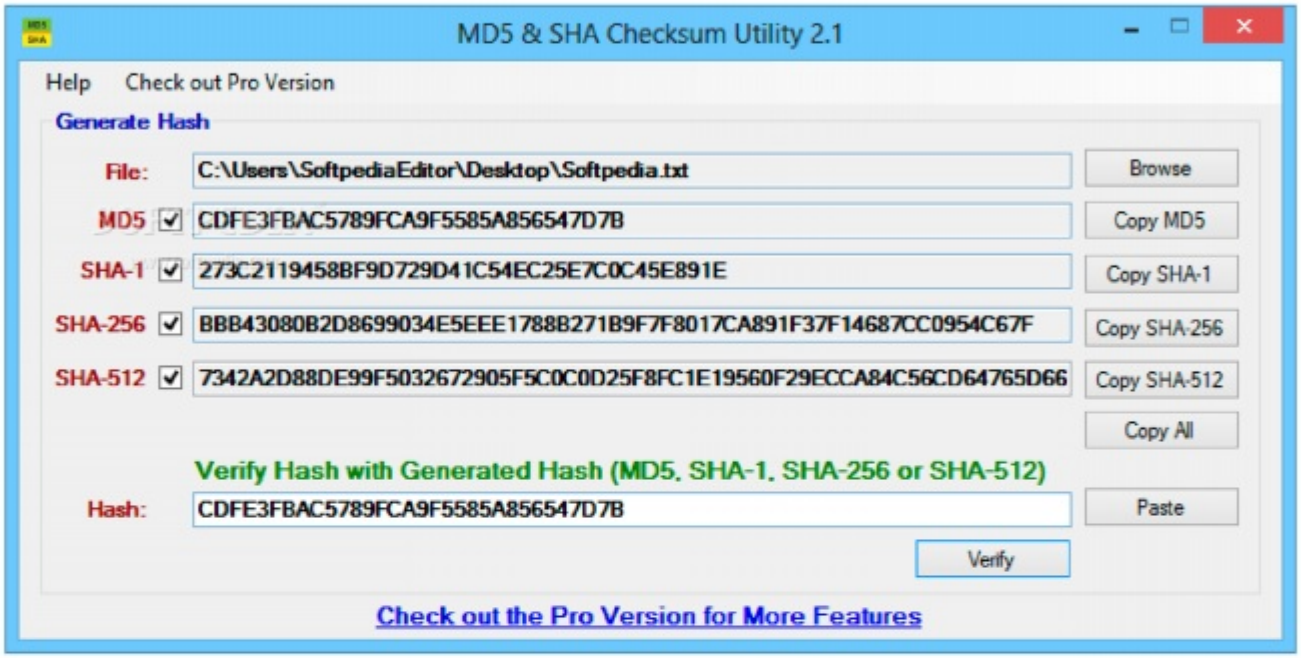
Все транзакции, произошедшие за определённый промежуток времени в системе, работающей на основе технологии BlockChain, записываются в блоки. Промежуток времени может быть любым, например, в криптовалюте LiteCoin это 2,5 мин., в BitCoin – 10 мин. Записанные блоки составляются в цепочку, где каждый последующий блок содержит в себе информацию о предыдущем блоке. Именно принцип выстраивания блоков информации в цепочку дал название технологии BlockChain.



Запись блоков происходит в регистрах у каждого участника системы. То есть в отличие от архитектуры «клиент-сервер», где все данные хранятся на одном/нескольких серверах, технология BlockChain является децентрализованной системой хранения данных. Ввиду того, что все данные дублируются у всех участников системы, в случае выхода из строя компьютера одного из участников, ни одна часть данных не будет потеряна. Чем больше участников задействовано в

той или иной системе на основе технологии BlockChain, тем выше надёжность сохранения информации.

В процессе работы, для каждого блока транзакций каждым из участников системы генерируется контрольная сумма – хеш. Хеш генерируется по определённому алгоритму. Наиболее часто используемые алгоритмы представлены ниже.



Предназначение хеша заключается в проверке подлинности информации в блоке. Например, вычислим SHA256-хеш для какой-либо фразы без точки и с точкой в конце фразы.

SHA256("The quick brown fox jumps over the lazy **dog**")

0x d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592

SHA256("The quick brown fox jumps over the lazy **dog.**")

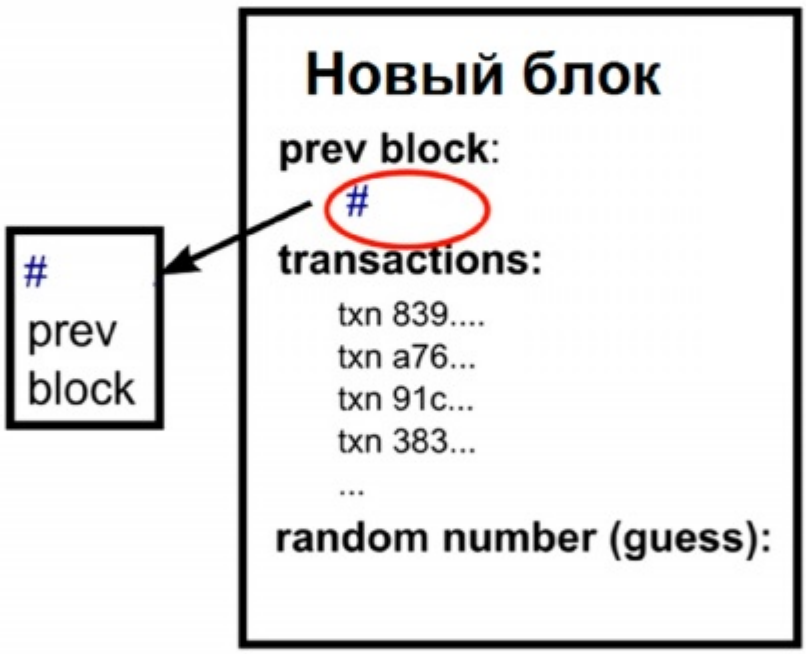
0x ef537f25c895bfa782526529a9b63d97aa631564d5d789c2b765448c8635fb6c

Мы видим, что добавление или изменение всего одного символа меняет сгенерированный SHA256-хеш полностью.

После генерации хеша каждый из участников системы отправляет хеш в систему другим участникам для сверки. Если хеш будет идентичен более чем у половины участников, то этот блок информации будет принят всеми участниками

системы как достоверный и записан в цепочку, в противном случае блок информации считается поддельным. Таким образом, для того чтобы с 50 % вероятностью подменить блок с недостоверными транзакциями, злоумышленнику необходимо иметь 50 % вычислительной мощности сети, только в таком случае блок может быть принят как достоверный. По сути один злоумышленник должен противостоять всей вычислительной мощности сети и чем больше сеть, тем меньше вероятности подделки блоков.

Ещё одним фактором защиты информации в технологии BlockChain является то, что блоки невозможно решать заранее: заранее решённый блок должен содержать в себе ссылку на предыдущий, ещё не собранный и не записанный блок.



Предсказать ссылку на один или несколько блоков вперёд невозможно, потому что ссылка также генерируется по алгоритму шифрования. Чтобы угадать хеш на ещё не существующий блок, одному компьютеру потребуется несколько лет, но когда блок транзакций уже собран, генерация хеша осуществляется за долю секунды.

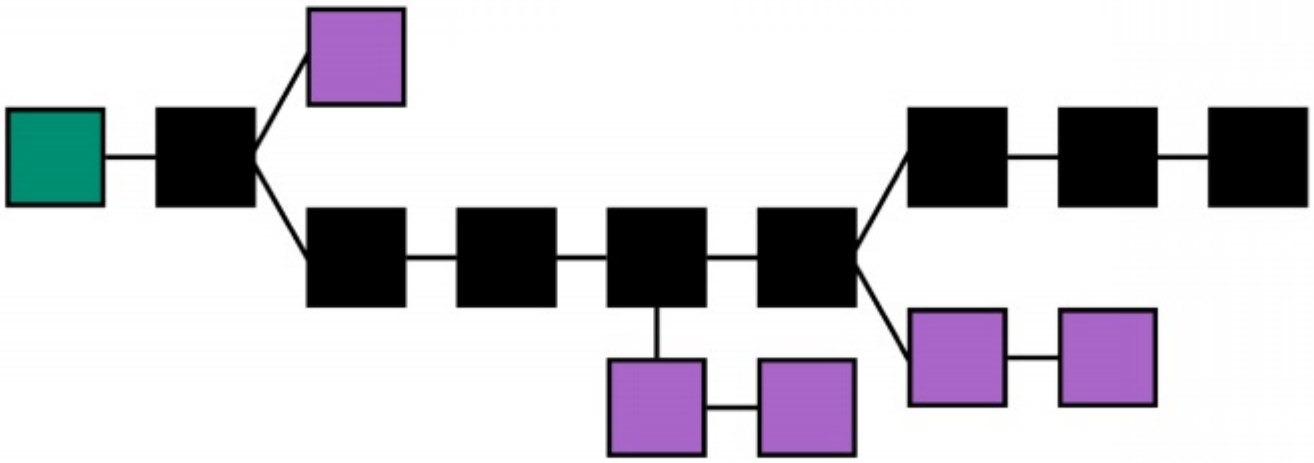
Таким образом, к преимуществам системы BlockChain можно отнести:

– Достоверность хранения данных. Чем больше участников системы, тем меньше вероятность подделки данных;

- Надёжность хранения данных. Копия всех данных хранится у каждого участника;
- Анонимность хранения данных. Несмотря на то, что данные присутствуют у всех участников, сами данные обезличены: например, участники системы BitCoin могут видеть только номер BitCoin-кошелька и суммы совершенных операций, но не могут видеть личность владельца кошелька и что именно приобреталось/продавалось с использованием этого BitCoin-кошелька.

К недостаткам технологии BlockChain можно отнести:

- Необходимость массива вычислительных мощностей;
- Огромные энергозатраты. Большое число участников, имеющих большие вычислительные мощности, требует колоссальных энегргозатрат;
- Неопределённый порядок создания блоков транзакций. Обмен транзакциями между участниками сети происходит неравномерно, поэтому не все участники всегда имеют одинаковый последний блок. Алгоритм выбора последнего блока задаётся в системе искусственно: выбирается наиболее длинная цепочка блоков, сформированная за промежуток времени после записи крайнего блока.



Записаны в цепочку будут блоки отмеченные чёрным цветом. Блоки, окрашенные фиолетовым цветом, будут отброшены, а находящиеся в них неподтверждённые транзакции – отправлены в очередь в следующие блоки.

- Система BlockChain всё же подвержена взлому. Вероятность подстановки недостоверного блока тем выше, чем выше доля вычислительной мощности злоумышленника в общей мощности сети.

Технология BlockChain по сути представляет собой новый тип систем организации базы данных, позволяющий широкой группе участников получать практически одновременный совместный доступ к общим данным.

BlockChain может использоваться как основа надёжного хранения данных в практически любых системах:

- в системах электронного голосования акционеров или политических выборов;
- в системах децентрализованных распределенных реестров (анонимное владение недвижимостью, земельными участками, банковскими счетами);
- в системах подтверждения авторства и права владения (реестр VIN-номеров, реестр прав на музыкальные произведения Soundchain.org);
- в системах учёта кредитных учреждений (Сбербанк в тестовом режиме запустил систему обмена валют на базе токенов; создан ориентированный на блокчейн-технологии банк Polybius);
- в системах Smart Contract (умный контракт), где выполнение каждого этапа контракта завязано на фиксировании в BlockChain-системе;
- как средство функционирования криптовалют.

Криптовалюты – наиболее широко известный пример использования технологии BlockChain. Теоретически «добыть» немного криптовалюты может каждый желающий: BitCoin или любая другая криптовалюта присуждаются как награда тому, кто первым решит математическую задачу по формированию блока, т.е. главным фактором получения награды является вычислительная мощность участника.

Для «добычи» необходимо обладать:

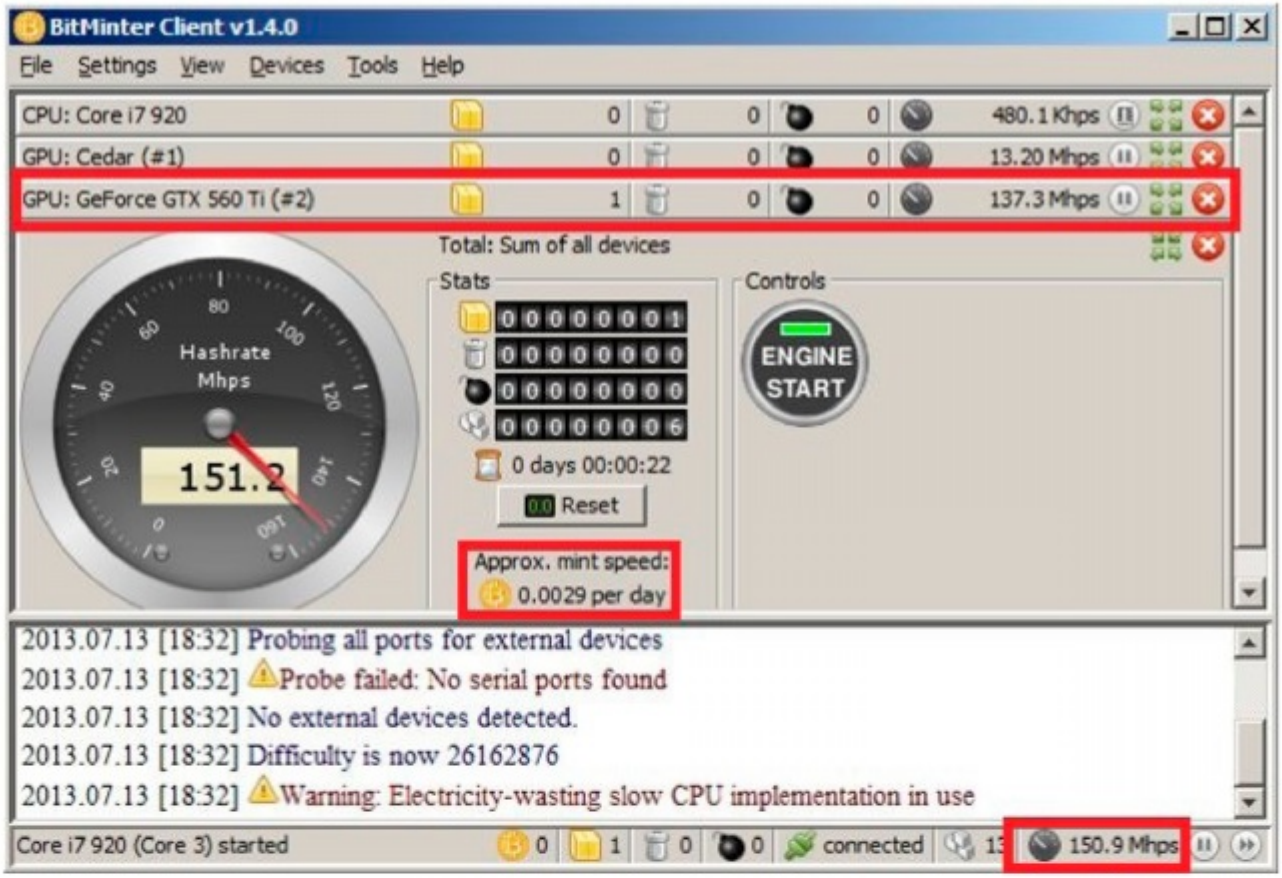
- программой-клиентом для участия в выбранной системе;
- любое вычислительное устройство;
- средства на обслуживание вычислительного устройства.

Под любым вычислительным устройством может подразумеваться хоть обычный компьютер, хоть несколько компьютеров с несколькими видеокартами (небольшая «ферма»), и даже сетевые хранилища (NAS). В конце 2016 г. Было раскрыто заражение 1 702 476 сетевых хранилищ вирусом-майнером, и не смотря

на то, что один NAS обладает ничтожной вычислительной мощностью, из-за огромного числа участвующих в майнинге устройств, злоумышленник «добывал» на свой кошелёк порядка 428 евро в сутки. Ниже представлено одно из устройств ботнета (bot net – сеть заражённых устройств), находящееся дома у ничего не подозревающего законного владельца, но при этом тихо добывающее криптовалюту для злоумышленника.

«Добычей» процесс называется по аналогии с добычей руды в шахтах – единицы ценности криптовалюты получаются благодаря работе по генерированию хешей, энергозатратам и течению времени. А участника системы, «добывающего» криптовалюту, называют «майнер» (англ. miner – шахтёр).

На нижепредставленной картинке мы видим пример программы для майнинга криптовалюты. Мы видим, что суммарная вычислительная мощность участника составляет 150,9 миллионов хешей в секунду, из них 137,3 миллионов хешей в секунду генерируется вычислительной мощностью видеокарты nVidia GTX 560 Ti. При этом приблизительная скорость добычи составляет 0,0029 единиц валюты BitCoin в день.



В криптовалютах ярко проявились все плюсы и минусы технологии BlockChain. Кроме того, добавились и некоторые другие проблемы:

- законодательный запрет на использование криптовалют в некоторых странах;
- ввиду того, что у криптовалют отсутствует подкрепление стоимости золотом, ценность и функционирование криптовалюты основывается исключительно на доверии участников;
- большой размер комиссий за ускорение проведения транзакций, либо очередь и длительное время подтверждения транзакций без комиссии;
- превышение допустимого размера блока. Так, например, в 2016 г. в криптовалюте BitCoin размер блока превысил установленный разработчиками размер 1 MB. Тогда BitCoin сообщество встало перед выбором: либо мириться с очередями неподтверждённых транзакций, либо увеличить размер блока. Увеличение размера блока потребовало написания новой версии программы-клиента, что поделило сообщество на два лагеря: те, кто использует традиционную версию BitCoin (BTC) и те, кто 1 августа 2017 г. перешли на форк (ответвление), названный «BitCoin Cash» (BCC);

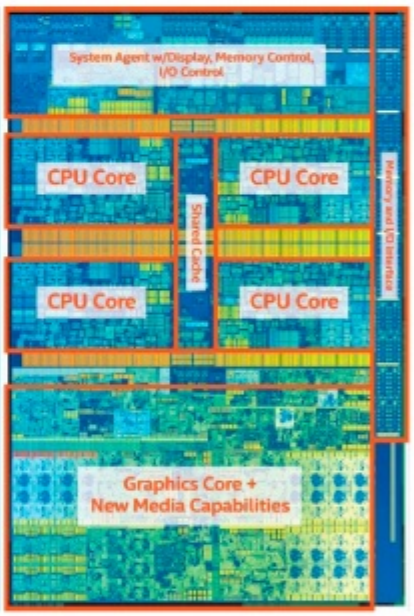
– владение бОльшей долей вычислительной мощности малой группой людей. По некоторым оценкам около 70% всей вычислительной мощности системы BitCoin принадлежит нескольким владельцам ферм, находящимся в Китае. Это обусловлено низкой стоимостью как на комплектующие для майнинга, так и на обслуживающую рабочую силу и на электроэнергию. Человек на картинке представленной ниже – это Chandler Guo, инвестор и владелец крупнейшей в мире BitCoin-фермы на фоне своего достояния. По некоторым оценкам эта ферма позволяла в год добывать BitCoin эквивалентно 8-ми миллионам долларов США, что объясняет довольную улыбку на лице этого азиата.

Появившаяся в 2009 г. криптовалюта BitCoin – самая известная, но далеко не единственная: на середину 2017 г. существует порядка 1 200 криптовалют отличающихся существенными параметрами системы – алгоритмом, позволяющим или не позволяющим использовать ASIC-майнеры, алгоритмом начисления награды, промежутком времени сборки блока транзакций и т.д.

Наиболее популярными являются криптовалюты:

- Ethereum;
- LiteCoin;
- Ripple;
- NXT;
- PeerCoin;
- NameCoin и др.

Изначально майнинг криптовалют производили на обычных компьютерах, с помощью центральных процессоров (CPU). Но поскольку процессор – штука хоть и мощная, но, чтобы обрабатывать все задачи, процессор должен быть универсальным и математический сопрцессор (ALU) занимает в центральном процессоре лишь малую часть.



Гораздо лучше для этих целей подходят видеокарты, а лучше несколько видеокарт. Причём, ввиду архитектурных особенностей, видеокарты на чипах nVidia для майнинга подходят лучше, чем карты на чипах AMD, хотя ещё год назад, до смены поколений видеокарт, ситуация была противоположной.

Производительность видеокарт, как и производительность математических сопроцессоров измеряется в количестве операций над дробными числами за секунду (FLoating-point Operations Per Second, FLOPS). Так, например, видеокарта nVidia GeForce GTX 1080 имеет производительность 9 триллионов операций с дробными числами за секунду (9 TFLOPS) при энергопотреблении 180 Вт.

Одна майниг-ферма из пяти таких карт будет потреблять 900 Вт (без учета остальных компонентов компьютера), а добыча криптовалюты будет сопровождаться огромными счетами за электроэнергию, покрываемыми, при высоком курсе, добытой криптовалютой.

Производители комплектующих увидев потребности майнеров представили на рынок «Mining Edition»-модификации своих видеокарт. На картинке ниже представлен Sapphire Radeon RX 470 Mining Edition.

В нём видеовыходы, как и остальные компоненты ответственные за вывод видеосигнала, упразднены не столько в целях удешевления, сколько для предотвращения дефицита производительных видеокарт на рынке путём разделения ниш спроса майнеров и геймеров.

Другие производители пошли еще дальше и предложили майнерам специализированные устройства – ASIC-майнеры (ASIC – application-specific integrated circuit, интегральная схема специального назначения).

Производительность ASIC-майнеров измеряется в количестве генерируемых хешей в секунду (HPS, hash per second), а соотношение их производительности к потребляемой мощности в разы превышает эффективность ферм из видеокарт: при энергопотреблении в 3-4 кВт/ч производительность одного ASIC-устройства достигает нескольких триллионов хешей в секунду.

На сегодняшний день майнинг в домашних условиях оправдан лишь для относительно новых криптовалют, только набирающих популярность: чем больше участвующих в майнинге той или иной валюты, тем больше сложность добычи и ниже вероятность получения награды. Более того, в некоторых системах награда майнерам снижается искусственно, например, в системе BitCoin раз в 4 года размер награды сокращался вдвое. Скачки курса криптовалюты также вносят свой вклад: падение курса многих криптовалют в июле 2017 г. в одночасье сделало майнинг на видеокартах нерентабельным, а вторичный рынок тотчас наполнился картами, использовавшимися для майнинга.

Однако, чтобы добывать криптовалюту вовсе не обязательно покупать дорогостоящее оборудование и отводить ему отдельное помещение. Многие организации предоставляют доступ к своим вычислительным мощностям за арендную плату. Информацию о таких сервисах можно легко найти в Интернет.